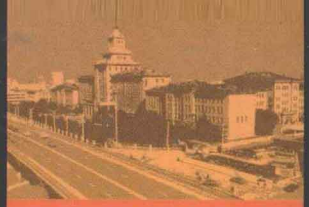
Elementary Number Theory (I)



HIT

数论经典著作系列

初等数论(I)

陈景润 著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

数论经典著作系列

Elementary Number Theory (I)

初等数论 (I)

陈景润 著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

数论是研究数的性质的一门学科。本书从科学实验的实际经验出发，分析了数论的发生、发展和应用，介绍了数论的初等方法。本书包含整数的性质、数的进位法、一部分不定方程和一次同余式及解法四章。每章后有习题，并在书末附有全部习题解答。本书写得深入浅出，通俗易懂，可供广大青年及科技人员阅读。

图书在版编目(CIP)数据

初等数论.1/陈景润著.—哈尔滨:哈尔滨工业大学出版社,2012.2

ISBN 978-7-5603-3495-0

Ⅰ.①初… Ⅱ.①陈… Ⅲ.①初等数论 Ⅳ.①O156.1

中国版本图书馆 CIP 数据核字(2012)第 014347 号

策划编辑 刘培杰 张永芹
责任编辑 尹 凡
封面设计 孙茵艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 黑龙江省教育厅印刷厂
开 本 787mm×1092mm 1/16 印张 8.5 字数 182 千字
版 次 2012 年 2 月第 1 版 2012 年 2 月第 1 次印刷
书 号 ISBN 978-7-5603-3495-0
定 价 18.00 元

哈尔滨工业大学出版社刘培杰数学工作室
已出版(即将出版)图书目录

书　名	出版时间	定　价	编号
新编中学数学解题方法全书(高中版)上卷	2007－09	38.00	7
新编中学数学解题方法全书(高中版)中卷	2007－09	48.00	8
新编中学数学解题方法全书(高中版)下卷(一)	2007－09	42.00	17
新编中学数学解题方法全书(高中版)下卷(二)	2007－09	38.00	18
新编中学数学解题方法全书(高中版)下卷(三)	2010－06	58.00	73
新编中学数学解题方法全书(初中版)上卷	2008－01	28.00	29
新编中学数学解题方法全书(初中版)中卷	2010－07	38.00	75
新编平面解析几何解题方法全书(专题讲座卷)	2010－01	18.00	61
数学眼光透视	2008－01	38.00	24
数学思想领悟	2008－01	38.00	25
数学应用展观	2008－01	38.00	26
数学建模导引	2008－01	28.00	23
数学方法溯源	2008－01	38.00	27
数学史话览胜	2008－01	28.00	28
从毕达哥拉斯到怀尔斯	2007－10	48.00	9
从迪利克雷到维斯卡尔迪	2008－01	48.00	21
从哥德巴赫到陈景润	2008－05	98.00	35
从庞加莱到佩雷尔曼	2011－08	138.00	136
从比勃巴赫到德·布朗斯	即将出版		
数学解题中的物理方法	2011－06	28.00	114
数学解题的特殊方法	2011－06	48.00	115
中学数学计算技巧	2012－01	48.00	116
中学数学证明方法	2012－01	58.00	117
数学趣题巧解	2012－03	28.00	128
数学奥林匹克与数学文化(第一辑)	2006－05	48.00	4
数学奥林匹克与数学文化(第二辑)(竞赛卷)	2008－01	48.00	19
数学奥林匹克与数学文化(第二辑)(文化卷)	2008－07	58.00	36
数学奥林匹克与数学文化(第三辑)(竞赛卷)	2010－01	48.00	59
数学奥林匹克与数学文化(第四辑)(竞赛卷)	2011－08	58.00	87

哈尔滨工业大学出版社刘培杰数学工作室
已出版(即将出版)图书目录

书　名	出版时间	定　价	编号
发展空间想象力	2010－01	38.00	57
走向国际数学奥林匹克的平面几何试题诠释(上、下)(第2版)	2010－02	98.00	63,64
平面几何证明方法全书	2007－08	35.00	1
平面几何证明方法全书习题解答(第2版)	2006－12	18.00	10
最新世界各国数学奥林匹克中的平面几何试题	2007－09	38.00	14
数学竞赛平面几何典型题及新颖解	2010－07	48.00	74
初等数学复习及研究(平面几何)	2008－09	58.00	38
初等数学复习及研究(立体几何)	2010－06	38.00	71
初等数学复习及研究(平面几何)习题解答	2009－01	48.00	42
世界著名平面几何经典著作钩沉——几何作图专题卷(上)	2009－06	48.00	49
世界著名平面几何经典著作钩沉——几何作图专题卷(下)	2011－01	88.00	80
世界著名平面几何经典著作钩沉(民国平面几何老课本)	2011－03	38.00	113
世界著名数论经典著作钩沉(算术卷)	2012－01	28.00	125
世界著名数学经典著作钩沉——立体几何卷	2011－02	28.00	88
世界著名三角学经典著作钩沉(平面三角卷Ⅰ)	2010－06	28.00	69
世界著名三角学经典著作钩沉(平面三角卷Ⅱ)	2011－01	28.00	78
世界著名初等数论经典著作钩沉(理论和实用算术卷)	2011－07	38.00	126
几何学教程(平面几何卷)	2011－03	68.00	90
几何学教程(立体几何卷)	2011－07	68.00	130
几何变换与几何证题	2010－06	88.00	70
几何瑰宝——平面几何500名题暨1000条定理(上、下)	2010－07	138.00	76,77
三角形的五心	2009－06	28.00	51
俄罗斯平面几何问题集	2009－08	88.00	55
俄罗斯平面几何5000题	2011－03	58.00	89
计算方法与几何证题	2011－06	28.00	129
463个俄罗斯几何老问题	2012－01	28.00	152
近代欧氏几何学	2012－2	38.00	162

哈尔滨工业大学出版社刘培杰数学工作室
已出版(即将出版)图书目录

书　名	出版时间	定　价	编号
超越吉米多维奇——数列的极限	2009－11	48.00	58
初等数论难题集(第一卷)	2009－05	68.00	44
初等数论难题集(第二卷)(上、下)	2011－02	128.00	82,83
谈谈素数	2011－03	18.00	91
平方和	2011－03	18.00	92
数论概貌	2011－03	18.00	93
代数数论	2011－03	48.00	94
初等数论的知识与问题	2011－02	28.00	95
超越数论基础	2011－03	28.00	96
数论初等教程	2011－03	28.00	97
数论基础	2011－03	18.00	98
数论入门	2011－03	38.00	99
解析数论引论	2011－03	48.00	100
基础数论	2011－03	28.00	101
超越数	2011－03	18.00	109
三角和方法	2011－03	18.00	112
谈谈不定方程	2011－05	28.00	119
整数论	2011－05	38.00	120
初等数论100例	2011－05	18.00	122
最新世界各国数学奥林匹克中的初等数论试题(上、下)	2012－01	138.00	144,145
算术探索	2011－12	158.00	148
初等数论(Ⅰ)	2012－01	18.00	156
初等数论(Ⅱ)	2012－01	18.00	157
初等数论(Ⅲ)	2012－01	28.00	158
组合数学浅谈	2012－02	18.00	159
同余理论	2012－02	38.00	163

哈尔滨工业大学出版社刘培杰数学工作室
已出版(即将出版)图书目录

书　　名	出版时间	定　价	编号
历届 IMO 试题集(1959—2005)	2006－05	58.00	5
历届 CMO 试题集	2008－09	28.00	40
历届国际大学生数学竞赛试题集(1994－2010)	2012－01	28.00	143
全国大学生数学夏令营数学竞赛试题及解答	2007－03	28.00	15
历届美国大学生数学竞赛试题集	2009－03	88.00	43
前苏联大学生数学竞赛试题及解答(上)	2012－03	28.00	169
前苏联大学生数学竞赛试题及解答(下)	2012－03	38.00	170
整函数	2012－1		161
俄罗斯函数问题集	2011－03	38.00	103
俄罗斯组合分析问题集	2011－01	48.00	79
博弈论精粹	2008－03	58.00	30
多项式和无理数	2008－01	68.00	22
模糊数据统计学	2008－03	48.00	31
受控理论与解析不等式	2012－03		165
解析不等式新论	2009－06	68.00	48
反问题的计算方法及应用	2011－11	28.00	147
建立不等式的方法	2011－03	98.00	104
数学奥林匹克不等式研究	2009－08	68.00	56
不等式研究(第二辑)	2012－02	68.00	153
初等数学研究(Ⅰ)	2008－09	68.00	37
初等数学研究(Ⅱ)(上、下)	2009－05	118.00	46,47
中国初等数学研究　2009 卷(第 1 辑)	2009－05	20.00	45
中国初等数学研究　2010 卷(第 2 辑)	2010－05	30.00	68
中国初等数学研究　2011 卷(第 3 辑)	2011－07	60.00	127
数阵及其应用	2012－02	28.00	164
不等式的秘密(第一卷)	2012－02	28.00	154
初等不等式的证明方法	2010－06	38.00	123
数学奥林匹克不等式散论	2010－06	38.00	124
数学奥林匹克不等式欣赏	2011－09	38.00	138
数学奥林匹克超级题库(初中卷上)	2010－01	58.00	66
数学奥林匹克不等式证明方法和技巧(上、下)	2011－08	158.00	134,135

哈尔滨工业大学出版社刘培杰数学工作室
已出版(即将出版)图书目录

书　名	出版时间	定　价	编号
500个最新世界著名数学智力趣题	2008－06	48.00	3
400个最新世界著名数学最值问题	2008－09	48.00	36
500个世界著名数学征解问题	2009－06	48.00	52
400个中国最佳初等数学征解老问题	2010－01	48.00	60
500个俄罗斯数学经典老题	2011－01	28.00	81
数学 我爱你	2008－01	28.00	20
精神的圣徒　别样的人生——60位中国数学家成长的历程	2008－09	48.00	39
数学史概论	2009－06	78.00	50
斐波那契数列	2010－02	28.00	65
数学拼盘和斐波那契魔方	2010－07	38.00	72
斐波那契数列欣赏	2011－01	28.00	160
数学的创造	2011－02	48.00	85
数学中的美	2011－02	38.00	84
最新全国及各省市高考数学试卷解法研究及点拨评析	2009－02	38.00	41
高考数学的理论与实践	2009－08	38.00	53
中考数学专题总复习	2007－04	28.00	6
向量法巧解数学高考题	2009－08	28.00	54
新编中学数学解题方法全书(高考复习卷)	2010－01	48.00	67
新编中学数学解题方法全书(高考真题卷)	2010－01	38.00	62
新编中学数学解题方法全书(高考精华卷)	2011－03	68.00	118
高考数学核心题型解题方法与技巧	2010－01	28.00	86
数学解题——靠数学思想给力(上)	2011－07	38.00	131
数学解题——靠数学思想给力(中)	2011－07	48.00	132
数学解题——靠数学思想给力(下)	2011－07	38.00	133
2011年全国及各省市高考数学试题审题要津与解法研究	2011－10	48.00	139
新课标高考数学——五年试题分章详解(2007～2011)(上、下)	2011－10	78.00	140,141
30分钟拿下高考数学选择题、填空题	2012－01	48.00	146
高考数学压轴题解题诀窍(上)	2012－02	78.00	166
高考数学压轴题解题诀窍(下)	2012－03	28.00	167
300个日本高考数学题	2012－03		142

哈尔滨工业大学出版社刘培杰数学工作室
已出版(即将出版)图书目录

书　名	出版时间	定　价	编号
中等数学英语阅读文选	2006－12	38.00	13
统计学专业英语	2007－03	28.00	16
方程式论	2011－03	38.00	105
初级方程式论	2011－03	28.00	106
Galois 理论	2011－03	18.00	107
代数方程的根式解及伽罗瓦理论	2011－03	28.00	108
线性偏微分方程讲义	2011－03	18.00	110
N 体问题的周期解	2011－03	28.00	111
代数方程式论	2011－05	28.00	121
动力系统的不变量与函数方程	2011－07	48.00	137
基于短语评价的翻译知识获取	2012－02	48.00	168
闵嗣鹤文集	2011－03	98.00	102
吴从炘数学活动三十年(1951～1980)	2010－07	99.00	32
吴振奎高等数学解题真经(概率统计卷)	2012－01	38.00	149
吴振奎高等数学解题真经(微积分卷)	2012－01	68.00	150
吴振奎高等数学解题真经(线性代数卷)	2012－01	58.00	151
钱昌本教你快乐学数学(上)	2011－12	48.00	155

联系地址:哈尔滨市南岗区复华四道街 10 号　哈尔滨工业大学出版社刘培杰数学工作室
网　　址:http://lpj.hit.edu.cn/
邮　　编:150006
联系电话:0451－86281378　　13904613167
E-mail:lpj1378@yahoo.com.cn

◎目录

整数的整除性

第1章

1.1 因数和倍数

我们把 $1,2,3,4,\cdots,n,\cdots$ 这些数叫做正整数，又叫做自然数，其中 $1,3,5,7,\cdots$ 叫做奇数；$2,4,6,8,\cdots$ 叫做偶数. 在整数范围内，很明显

正整数+正整数=正整数

正整数×正整数=正整数

但是由正整数减去正整数，得到的可能是正整数，也可能不是正整数.

$$-1,-2,-3,-4,\cdots,-n,\cdots$$

这些数叫做负整数，而正整数和负整数再加上零，就统一叫做整数.

在整数范围内，我们有

整数+整数=整数

整数−整数=整数

整数×整数=整数

但是整数除整数不一定是整数，究竟什么样的整数除什么样的整数才能得整数呢？研究这个问题，就是研究整数的整除性.

以后,如果没有特别声明,我们将用

$$a,b,c,d,\cdots$$

等英文字母表示整数. 当几个字母写在一起时,表示将这几个字母相乘起来. 例如

$$ab = a \times b, abc = a \times b \times c$$

$$abcd = a \times b \times c \times d$$

等. 但注意数目字写在一起时不表示相乘,例如 55 不是 5×5 而是五十五,234 不是 $2 \times 3 \times 4$ 而是二百三十四. 而当数目字和字母写在一起时,则表示这个数目字和字母相乘. 例如 $2a = 2 \times a, 15a = 15 \times a, 99abc = 99 \times a \times b \times c, 1234abcd = 1234 \times a \times b \times c \times d$.

我们还使用记号 $(-a)$ 来表示 $-a$,即 $(-a) = -a$,又有 $(-a)(-b) = (-a) \times (-b), (-a)b = (-a) \times b, a(-b) = a \times (-b)$.

定义 1 设 a,b 是整数,$b \neq 0$. 如果有一个整数 c,它使得 $a = bc$,则 a 叫做 b 的倍数,b 叫做 a 的因数. 我们有时说,b 能整除 a 或 a 能被 b 整除;也有时说,b 能除尽 a,或 a 能被 b 除尽.

如果 b 能整除 a,我们就用 $b \mid a$ 这个符号来表示它,例如 $2 \mid 4, 3 \mid 6$. 由于 $-30 = 6 \times (-5), 20 = (-5) \times (-4)$,所以 $6 \mid (-30), (-5) \mid 20$.

如果 b 不能整除 a,我们就写作 $b \nmid a$,例如 $2 \nmid 3, 3 \nmid 8, (-3) \nmid 5, (-5) \nmid 12$.

如果 a 是一个整数,$a \neq 0$,而 m 是一个正整数,则由于 $0 = a \times 0, ma = a \times m, -ma = a \times (-m)$,所以 $0, ma$ 和 $-ma$ 都是 a 的倍数,即

$$0,a,2a,3a,4a,\cdots$$

都是 a 的倍数,而

$$-a, -2a, -3a, -4a,\cdots$$

也都是 a 的倍数,我们使用记号 $|a|$ 来表示

$$|a| = \begin{cases} a & \text{当 } a \geqslant 0 \\ -a & \text{当 } a < 0 \end{cases}$$

我们把 $|a|$ 叫做 a 的绝对值,例如 $|2| = |-2| = 2, |5| = |-5| = 5$.

引理 1 如果 a,b 是两个整数,而 $a \mid b$,则

$$(-a) \mid b, a \mid (-b), (-a) \mid (-b), |a| \mid |b|$$

证 因为 $a \mid b$,所以由定义 1 有一个整数 c,它使得 $b = ac$,故得

$$b = (-a)(-c), -b = a(-c) = (-a)c$$

$$|b| = |ac| = |a||c|$$

由于 $a,b,c, -a, -b, -c, |a|, |b|$ 和 $|c|$ 都是整数,所以有

$$(-a) \mid b, a \mid (-b), (-a) \mid (-b), |a| \mid |b|$$

引理 2 如果 a,b,c 都是整数而 $a \mid b, b \mid c$,则有 $a \mid c$.

证 因为 $a \mid b$,所以由定义 1 有一个整数 d,它使得 $b = ad$. 又由于 $b \mid c$,所以有一个整数 e 它使得 $c = be$. 由 $c = be$ 和 $b = ad$ 有 $c = ade$. 由于 d 和 e 都是整数,所以 de 也是整数. 由定义 1 和 $c = ade$ 有 $a \mid c$.

引理 3 如果 a,b 都是整数而 $|a| < |b|, |b| \mid |a|$,则有

$$a = 0$$

证 因为 $|b| \mid |a|$,所以由定义 1 有一个整数 c,它使得 $|a| = |b|c$. 如果 $|a| = 0$,则有 $a = 0$. 如果 $|a| > 0$,则由 $0 < |a| < |b|$ 和 $|a| = |b|c$ 有 $c \geqslant 0$. 如果 $c > 0$,则由于 c 是整数而有 $c \geqslant 1$. 由 $|a| = |b|c$ 和 $c \geqslant 1$ 有 $|a| \geqslant |b|$,这和 $|a| < |b|$ 发生矛盾,所以有 $c = 0$. 由 $c = 0$ 和 $|a| = |b|c$ 有 $a = 0$.

引理 4 如果 a,b 是两个整数,$b \neq 0$,则一定有并且只有两个整数 q,r,可使

$$a = bq + r, 0 \leqslant r < |b|$$

成立.

证 如果 $b > 0$,则 b 的倍数当从负数到正数,由小到大列出时是

$$\cdots, -4b, -3b, -2b, -b, 0, b, 2b, 3b, 4b, \cdots$$

如果 $b < 0$,则 b 的倍数当从负数到正数,由小到大列出时是

$$\cdots, 4b, 3b, 2b, b, 0, -b, -2b, -3b, -4b, \cdots$$

现在有两种可能:

(1) 存在有一个整数 q,使得 $a = bq$,故 $r = 0$. 本引理成立.

(2) 当 $b > 0$ 时,存在有一个整数 q,使得 $qb \leqslant a < (q+1)b$. 而当 $b < 0$ 时,存在有一个整数 q,使得 $qb \leqslant a < (q-1)b$,故有 $a = bq + r$,而 $0 \leqslant r < |b|$.

现在要来证明只有唯一的这样一对 q,r,使得 $a = bq + r, 0 \leqslant r < |b|$ 成立,假设还有另外一对 q_1, r_1,可使

$$a = bq_1 + r_1, 0 \leqslant r_1 < |b|$$

成立,那么将上面的二个关系式相减,得

$$0 = b(q - q_1) + (r - r_1)$$

也就是 $-b(q - q_1) = r - r_1$,所以由定义 1 有 $b \mid (r - r_1)$. 再根据引理 1 得 $|b| \mid |r - r_1|$. 因为 $0 \leqslant r < |b|, 0 \leqslant r_1 < |b|$,所以有

$$|r - r_1| = \begin{cases} r - r_1 \leqslant r < |b| & \text{当 } r \geqslant r_1 \text{ 时} \\ r_1 - r \leqslant r_1 < |b| & \text{当 } r < r_1 \text{ 时} \end{cases}$$

由 $|r - r_1| < |b|, |b| \mid |r - r_1|$ 和引理 3 得到 $r - r_1 = 0$,也就是 $r = r_1$. 由 $b \neq 0$ 和 $b(q - q_1) = r_1 - r = 0$ 得到 $q - q_1 = 0$,也就是 $q = q_1$.

1.2 素数和复合数

1 这个数只有一个正因数,就是它本身,任何大于 1 的正整数 a 都最少有二个正因数,就是 1 和 a.

2 只能被 1 和 2 整除,不能被其他正整数整除,同样 3 只能被 1 和 3 整除,不能被其他正整数整除. 我们说 2 是素数,3 也是素数.

4 除了能被 1 和 4 整除,还能被 2 整除. 6 除了能被 1 和 6 整除,还能被 2 和 3 整除. 我们说 4 是复合数,6 也是复合数.

定义 2 一个大于 1 的正整数,只能被 1 和它本身整除,不能被其他正整数整除,这样的正整数叫做素数(有的书上叫做质数).

例如 2,3,5,7,11,13,17,19 都是素数.

以后我们将常用 p 或 $p_1, p_2, p_3, \cdots$ 表示素数.

定义 3 一个正整数除了能被 1 和本身整除以外,还能被另外的正整数整除,这样的正整数叫做复合数.

例如 4,6,8,9,10,12,14,15,16,18,20 都是复合数.

由素数与复合数的定义可知,全体正整数可分为三类:

(1)1 这个数.

(2) 全体素数.

(3) 全体复合数.

当然有无限多的复合数,比如大于 2 的偶数

$$4,6,8,10,12,\cdots$$

都是复合数.

定义 4 如果一个正整数 a 有一个因数 b,而 b 又是素数,则 b 就叫做 a 的素因数.

例如 $12 = 3 \times 4$,所以 3 和 4 都是 12 的因数,由于 3 是素数而 4 不是素数,所以 3 是 12 的素因数而 4 不是 12 的素因数.

引理 5 如果 a 是一个大于 1 的整数,则 a 的大于 1 的最小因数一定是素数.

证 如果 a 是一个素数,则 a 的大于 1 的因数只有一个,就是 a,所以 a 的大于 1 的最小因数就是素数 a.

如果 a 是复合数,则 a 除 1 和 a 外一定有其他的正因数. 假设 b 是这些正因数中的最小的,我们将证明 b 不是复合数而是素数. 先假定 b 不是素数而是复合数,则由于 b 是复合数,所以 b 一定有大于 1 而不等于 b 的因数 c. 由 $c \mid b, b \mid a$

和引理2有 $c \mid a$,即 c 是 a 的因数,又有 $1 < c < b$,这与假设 b 是 a 的大于1的最小因数矛盾. 所以 b 不是复合数而是素数. 因此 a 的大于1的最小的因数 b 是素数.

这个引理说明了:任何大于1的整数都至少有一个素因数.

观察一个正整数 a 是不是素数,是否得用小于 a 大于1的整数一一来试除呢? 不用.

引理6 如果 a 是一个大于1的整数,而所有 $\leqslant \sqrt{a}$ 的素数都除不尽 a,则 a 是素数.

证 首先证明,如果 a 被 > 1 而 $\leqslant \sqrt{a}$ 的整数都除不尽,则 a 是素数. 假设 a 是复合数而 $a = bc$,其中 b 和 c 都是大于1的整数. 由于 a 被 > 1 而 $\leqslant \sqrt{a}$ 的整数都除不尽,所以由 $b > \sqrt{a}, c > \sqrt{a}$,而得 $bc > \sqrt{a} \cdot \sqrt{a} = a$,这与 $bc = a$ 是矛盾的,所以如果 a 被 > 1 而 $\leqslant \sqrt{a}$ 的整数都除不尽,则 a 就是素数.

由上可知如果 a 是复合数,则 a 一定有 > 1 而 $\leqslant \sqrt{a}$ 的因数. 而由引理5知 a 的大于1的最小因数一定是素数,故本引理得证.

假设 $n \geqslant 2$ 是一个整数,定义

$$a_1 a_2 \cdots a_n = \begin{cases} a_1 a_2 & \text{当 } n = 2 \text{ 时} \\ a_1 a_2 a_3 & \text{当 } n = 3 \text{ 时} \\ a_1 a_2 a_3 a_4 & \text{当 } n = 4 \text{ 时} \\ a_1 a_2 a_3 a_4 \cdots a_n & \text{当 } n \geqslant 5 \text{ 时} \end{cases}$$

引理7 有无限多个素数.

证 假设素数的个数是有限多个,共有 n 个,就是 $p_1, p_2, p_3, \cdots, p_n$. 其中 $p_1 = 2, p_2 = 3, p_3 = 5, \cdots$. 令 $a = p_1 \cdots p_n + 1$,如果 a 是素数,则因 a 不等于 $p_1, p_2, \cdots, p_n$ 中的任何一个,故素数的个数最少有 $n + 1$ 个而与假设素数的个数共有 n 个矛盾. 如果 a 不是素数,则由引理5知道 a 的大于1的最小因数 b 是素数. 由于 $p_1 \cdots p_n$ 被 $p_1, p_2, \cdots, p_n$ 中的任何一个素数都除尽,但1被 $p_1, p_2, \cdots, p_n$ 中的任何一个素数都除不尽,所以 a 被 $p_1, p_2, \cdots, p_n$ 中的任何一个素数都除不尽. 因此 b 不等于 $p_1, \cdots, p_n$ 中的任何一个素数,故在 $p_1, \cdots, p_n$ 以外还有素数.

1.3 素数分布的简单概况

素数的分布情况是数论中最有趣味的一个分支,其中的推测和定理,很多都是先由经验得到的. 现有的最完善的素数表是查基尔(Don Zagier)作的,他把不大于50 000 000的素数都列出了. (见The Mathematical Intelligencer,1977

年8月号)

根据这个素数表可以查出素数的分布有下列情况:

在1到100中间有25个素数,

在1到1 000中间有168个素数,

在1 000到2 000中间有135个素数,

在2 000到3 000中间有127个素数,

在3 000到4 000中间有120个素数,

在4 000到5 000中间有119个素数,

在5 000到10 000中间有560个素数.

所以这些数字提示我们素数的分布,越往上越稀. 我们将5 000以内的素数表附在本章之末. 到目前为止所知道的最大素数是$2^{19\,937}-1$. 在证明$2^{19\,937}-1$是一个素数时需借助于电子计算机并用特殊方法. 我们有

$$2^{19\,937}-1 > 10^{6\,001}$$

关于素数的分布有许多问题,有的已经解决了,有的直到现在还没有解决.

首先的问题是关于素数的个数问题.

在数论里经常用$\pi(x)$表示不大于x的素数的个数. 所以$\pi(3)=2$,$\pi(100)=25$,$\pi(1\,000)=168$.

现在就几个不很大的x把相应的$\pi(x)$,$\frac{x}{\log x}$和它们的比值列表如下:

x	$\pi(x)$	$\frac{x}{\log x}$	$\frac{\pi(x)}{\frac{x}{\log x}}$	$\frac{\pi(x)}{x}$
1 000	168	144.764…	1.160 5…	0.168 0
2 000	303	263.126…	1.151 5…	0.151 5
5 000	669	587.047…	1.139 6…	0.133 8
10 000	1 229	1 085.73	1.131 9…	0.122 9
50 000	5 133	4 621.166…	1.110 7…	0.102 66
100 000	9 592	8 685.889…	1.104 3…	0.095 92

这个表提示我们三点:

(1) 有无限多个素数.

(2) 当x越大时,$\pi(x)$与$\frac{x}{\log x}$的比值越接近1.

(3) 当x越大时,$\pi(x)$与x的比值越接近0.

阿达马(Hadamard)和德·拉·瓦莱·普森(De la Vallée Poussin)各自独立地在1896年证明了素数定理,即